

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEIZURE OF:)

)
)
)
INTERNAL CITIBANK ACCOUNT) 1:24-sw-639
HOLDING THE BALANCE OF)
#9250974043)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250974523)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250975619)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250977018)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250972814)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250977565)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9111716029)
)
INTERNAL CITIBANK ACCOUNT)
HOLDING THE BALANCE OF)
#9250969228)
)
INTERNAL TD BANK ACCOUNT) 1:24-sw-640
HOLDING THE BALANCE OF)
#4441079377)
)
INTERNAL TD BANK ACCOUNT)

HOLDING THE BALANCE OF #4408454356)))	
INTERNAL TD BANK ACCOUNT HOLDING THE BALANCE OF #4408376617)))	
UP TO \$28,400 IN AN INTERNAL TD BANK ACCOUNT HOLDING THE BALANCE OF #4441223776)))	
INTERNAL TD BANK ACCOUNT HOLDING THE BALANCE OF #4408354192)))	
INTERNAL JP MORGAN CHASE ACCOUNT HOLDING THE BALANCE OF #550635711)))	1:24-sw-641
INTERNAL JP MORGAN CHASE ACCOUNT HOLDING THE BALANCE OF #575850907)))	
INTERNAL BANK OF AMERICA ACCOUNT HOLDING THE BALANCE OF #435048231338)))	1:24-sw-642
INTERNAL TRUIST ACCOUNT HOLDING THE BALANCE OF #1470014663126)))	1:24-sw-643
INTERNAL TRUIST ACCOUNT HOLDING THE BALANCE OF #1470013063435)))	
INTERNAL TRUIST ACCOUNT HOLDING THE BALANCE OF #1470013876622)))	
INTERNAL TRUIST ACCOUNT HOLDING THE BALANCE OF # 1210007787810)))	

AFFIDAVIT IN SUPPORT OF WARRANTS TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, Samantha Wendt, being duly sworn, hereby, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since June of 2023. I am currently assigned to the Washington Field Office. My primary duties include investigating violations of federal law, including securities fraud, wire fraud, bank fraud, and internet-enabled crimes. Part of those duties include investigating instances of wire fraud and bank fraud being used for financial gain at the expense of others. Before my career as an FBI Special Agent, I was employed as a Forensic Accountant by the FBI in the Seattle Field Office for two years. As part of that role, I conducted the financial portion of investigations, which included reviewing financial records and determining the sources and uses of funds. I have participated in numerous investigations related to financial crimes and have experience analyzing financial documents, interviewing suspects and witnesses, and reviewing evidence obtained from physical and digital search warrants.

2. This affidavit is based on my personal investigation and the investigation of others, including federal and local law enforcement officials whom I know to be reliable. The facts and information contained in this affidavit are based upon witness interviews and my review of records, documents, and other physical evidence obtained during this investigation. This affidavit does not include each and every fact known to the government, but only those facts necessary to establish probable cause to support the issuance of the seizure warrant.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that

the property set forth in the “Assets to be Seized” section of this affidavit are the proceeds of wire fraud, in violation of 18 U.S.C. § 1343, and mail fraud, in violation of 18 U.S.C. 1341. The proceeds of wire fraud and mail fraud are subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and are subject to criminal forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as incorporated by 28 U.S.C. § 2461(c).

ASSETS TO BE SEIZED

4. The assets to be seized are as follows (hereafter referred to as the “**SUBJECT ACCOUNTS**”):

- a. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250974043 (“**SUBJECT ACCOUNT 1**”), held in the name of S&W Façade Management Inc;
- b. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250974523 (“**SUBJECT ACCOUNT 2**”), held in the name of Carson Truck Service Inc;
- c. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250975619 (“**SUBJECT ACCOUNT 3**”), held in the name of Pure Life HL Inc;
- d. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250977018 (“**SUBJECT ACCOUNT 4**”), held in the name of BHB Products Trading Inc;
- e. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250972814 (“**SUBJECT ACCOUNT 5**”), held in the

name of Leslie Cell Phone Accessories Inc;

- f. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250977565 (“**SUBJECT ACCOUNT 6**”), held in the name of LT Restaurant Supplies Inc;
- g. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9111716029 (“**SUBJECT ACCOUNT 7**”), held in the name of Phenix Beauty Supplies Inc;
- h. All funds being held in an internal Citibank Account holding the balance of Citibank Account #9250969228 (“**SUBJECT ACCOUNT 8**”), held in the name of Kim Fashionable Clothing Inc;
- i. All funds being held in an internal TD Bank Account holding the balance of TD Bank Account #4441079377 (“**SUBJECT ACCOUNT 9**”), held in the name of SSW Investment Inc;
- j. All funds being held in an internal TD Bank Account holding the balance of TD Bank Account #4408454356 (“**SUBJECT ACCOUNT 10**”), held in the name of Above and Beyond Heating Corp;
- k. All funds being held in an internal TD Bank Account holding the balance of TD Bank Account #4408376617 (“**SUBJECT ACCOUNT 11**”), held in the name of Kim Fashionable Clothing Inc;
- l. Up to \$28,400 being held in an internal TD Bank Account holding the balance of TD Bank Account #4441223776 (“**SUBJECT ACCOUNT 12**”), held in the name of UJS Equipment Inc;

- m. All funds being held in an internal TD Bank Account holding the balance of TD Bank Account #4408354192 (“**SUBJECT ACCOUNT 13**”), held in the name of LMH Computer Service Inc;
- n. All funds being held in an internal JP Morgan Chase Account holding the balance of JP Morgan Chase Account #550635711 (“**SUBJECT ACCOUNT 14**”), held in the name of Pure Life HL Inc;
- o. All funds being held in an internal JP Morgan Chase Account holding the balance of JP Morgan Chase Account #575850907 (“**SUBJECT ACCOUNT 15**”), held in the name of Chia Supplies Co Limited;
- p. All funds being held in an internal Bank of America Account holding the balance of Bank of America Account #435048231338 (“**SUBJECT ACCOUNT 16**”), held in the name of Lena Castle Inc;
- q. All funds being held in an internal Truist Account holding the balance of Truist Account #1470014663126 (“**SUBJECT ACCOUNT 17**”), held in the name of BHB Products Trading Inc;
- r. All funds being held in an internal Truist Account holding the balance of Truist Account #1470013063435 (“**SUBJECT ACCOUNT 18**”), held in the name of Amcor Plus One Wholesale Inc;
- s. All funds being held in an internal Truist Account holding the balance of Truist Account #1470013876622 (“**SUBJECT ACCOUNT 19**”), held in the name of Chia Supplies Co Limited;
- t. All funds being held in an internal Truist Account holding the balance of

Truist Account #1210007787810 (“**SUBJECT ACCOUNT 20**”), held in the name of UJS Equipment Inc;

LEGAL AUTHORITY

5. 18 U.S.C. § 1341 (mail fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, by placing in an authorized depository for delivery by mail, by taking or receiving from an authorized depository for mail, by causing to be delivered by mail or by any private or commercial interstate carrier, and by depositing or causing to be deposited to be sent or delivered by any private or commercial interstate-carrier for the purpose of executing such scheme or artifice.

6. 18 U.S.C. § 1343 (wire fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

7. 18 U.S.C. § 981(a)(1)(C) (forfeiture for specified unlawful activities) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity (“SUA”), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S.

Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

8. 28 U.S.C. § 2461(c) (civil to criminal forfeiture incorporation statute) provides that if a person is charged in a criminal case with a violation for which the civil or criminal forfeiture of property is authorized, the government may include notice of the forfeiture in the charging instrument pursuant to the Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to forfeiture, the Court shall order forfeiture of the property as part of the defendant's sentence. The procedures of 21 U.S.C. § 853 shall apply to all stages of a criminal forfeiture proceeding, except for subsection (d) of that statute.

9. 18 U.S.C. § 981(b)(3) (civil seizures) provides that notwithstanding the provisions of Fed. R. Crim. P. 41(a), a seizure warrant issued pursuant to that subsection by a judicial officer in any district in which a forfeiture action against the property to be seized may be brought, and may be executed in any district in which the property to be seized is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or international agreement.

10. 21 U.S.C. § 853(f) (criminal seizures) provides that the government may request a seizure warrant authorizing the seizure of property subject to forfeiture in the same manner as for a search warrant. The seizure warrant issues if the Court determines that there is probable cause to believe that the property seized would, in the event of conviction, be subject to forfeiture and that a restraining order may not be sufficient to assure the availability of such property for forfeiture.

11. A restraining order would be inadequate to preserve the bank accounts for forfeiture. Based on my training and experience, I know that restraining orders served on banks

sometimes fail to preserve the property for forfeiture because the bank representative receiving the restraining order fails to put the necessary safeguards in place to freeze the money in time to prevent the account holder from accessing the funds electronically, or fails to notify the proper personnel as to the existence of the order.

12. Under 18 U.S.C. § 984, for any forfeiture action *in rem* in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

- a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;
- b. It is not a defense that those funds have been removed and replaced by other funds; and
- c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the “guilty” property had been kept. The statute does not, however, allow the government to reach back in time for an unlimited period. A forfeiture action (including a seizure) against property not directly traceable to the offense that is the basis for the forfeiture cannot be commenced more than one year from the date of the offense.

PROBABLE CAUSE

THE SCHEME TO DEFRAUD

14. The FBI, the Treasury Inspector General for Tax Administration (“TIGTA”), and the United States Postal Inspection Service (“USPIS”) (collectively, the “Joint Investigation”),

are investigating a conspiracy which exploits the Internal Revenue Service's ("IRS") Modernized Internet Employer Identification Number ("Mod IEIN") online portal. Mod IEIN is the IRS system that allows users to register for a unique Employer Identification Number ("EIN") for a business. These transactions are processed at IRS Enterprise Computing Centers located in West Virginia and Tennessee, making each of these transactions an interstate wire communication.

15. The investigation shows that Fei LIANG ("LIANG"), Ziguang LI ("LI"), and others obtained EINs for various businesses in furtherance of a scheme to defraud. These EINs allowed the co-conspirators to open business bank accounts¹ at various financial institutions for the purpose of receiving fraudulent wire transfers. Through victim interviews and the review of complaints submitted to the FBI's Internet Crime Complaint Center ("IC3"),² law enforcement has determined that many of these wire transfers were the result of a tech support scam³ targeting older adults. The proceeds of this fraudulent activity were rapidly withdrawn or moved between bank accounts controlled by different co-conspirators. This rapid movement of funds is

1 From training and experience, I know that fraudsters often prefer business bank accounts for schemes involving high dollar transactions. This is due to the perception that banks apply greater scrutiny to large deposits when they are credited to personal bank accounts.

2 IC3 is an FBI-led program that allows victims of cyber-crime to file formal complaints. These complaints are made available to federal, state, local, or international law enforcement as appropriate.

3 From training and experience, I know that tech support scams typically involve a fraudster who impersonates an employee of a legitimate technology company (e.g., Microsoft) and offers to "fix" a non-existent problem on the victim's computer. The fraudster will often trick the victim into (1) giving the fraudster access to the victim's financial accounts (2) installing malicious software on the victim's computer, and/or (3) giving the fraudster remote access to the victim's computer. According to the National Council on Aging's website "In 2020, at least 66% of tech support scam victims were age 60 or older."

indicative of communication and coordination between various individuals in furtherance of the conspiracy.

16. On July 25, 2024, a grand jury indicted LIANG and LI on one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) and six counts of concealment money laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 2.(Case No. 1:24-cr-170). It further alleged that the specified unlawful activity is wire fraud, in violation of 18 U.S.C. § 1343, and mail fraud, in violation of 18 U.S.C. § 1341.

The Source of Funds: Elder Fraud Scams

17. The investigation revealed a conspiracy that targeted unsuspecting victims through a nationwide tech support scam. Typically, the victims reported receiving a pop-up on their computer. The pop-ups included a phone number to contact for assistance. Once the victims called the phone number, the victim was advised to provide the purported technical support individual access to their computer. Upon doing so, the victim was often informed that their bank account had been hacked and the victim needed to secure their financial assets by transferring their money to the bank accounts associated with the conspiracy. The victim—believing they were sending money to address real issues with their computer and bank accounts—either wired money to bank accounts controlled by LIANG and coconspirators or mailed checks to coconspirators to be deposited into conspirator-controlled bank accounts.

The Fictitious Virginia Business Entities

18. On June 16, 2023, Dragon Auto Parts Inc. was incorporated by the Commonwealth of Virginia State Corporation Commission (“SCC”) with a registered agent of B.P. and registered office address of 7630 Little River Turnpike, Ste 720-10, Annandale,

Virginia 22003 (“7630 Little River Turnpike”). 7630 Little River Turnpike is associated with LocalWorks, which is a company that rents office space to individuals and businesses. The investigation revealed that LocalWorks had no records involving B.P. or Dragon Auto Parts Inc. renting office space.

19. On June 21, 2023, TD Bank account number xxxxxx6540 for Dragon Auto Parts Inc. (EIN: 93-1915932) was opened at a location in the Eastern District of Virginia. Included in the TD Bank account opening documents was a Dominion Energy customer bill for an identity theft victim identified here as “B.P.” showing an address of 1515 Richmond Hwy, Unit 906, Arlington, Virginia 22202 (“1515 Richmond Hwy”) dated June 5, 2023.

20. Records from Dominion Energy indicated that they were unable to locate an account associated with B.P., 1515 Richmond Hwy, or the meter number provided in Dominion Energy customer bill. Further, 1515 Richmond Hwy is associated with Crystal Square Apartments. Crystal Square Apartments had no records involving B.P. or Dragon Auto Parts Inc. renting Unit 906 in 2023. I reviewed bank surveillance footage associated with the June 21, 2023 bank account opening for TD Bank xxxxxx6540.

21. Two photographs obtained from the June 21, 2023 TD Bank surveillance footage reviewed are displayed below:



22. I have compared the photographs above with known images of LIANG. Based on that review and my training and experience, I believe the person depicted above to be LIANG.

23. Between June 26, 2023 and July 13, 2023, TD Bank account number xxxxxx6540 was the beneficiary of two wire transfers and one cashier's check deposit totaling over \$139,000. These deposits included a \$39,221.01 wire transfer from Victim-1's M&T Bank account on July 13, 2023. On March 4, 2024, I interviewed a 74-year-old resident of Connecticut (identified here as "Victim-1") who verified that the wire transfer from Victim-1's M&T Bank account to TD Bank xxxxxx6540 was the result of a tech support scam.

24. Further investigation revealed that business bank accounts were opened for Dragon Auto Parts Inc. (using EIN 93-1915932 and B.P.'s identity) at other financial institutions, including PNC, Truist, Citibank, Wells Fargo, and United Bank. Account opening documents associated with the Wells Fargo account in the name of Dragon Auto Parts Inc. indicated the business had five employees and was described as "Tire Shop and Automotive Parts." Financial analysis revealed no deposits or withdrawals consistent with an automotive business.

25. Between June 26, 2023 through October 17, 2023, the bank accounts described above, all opened in the name of Dragon Auto Parts Inc., were the beneficiary of 19 wire transfers and one cashier's check deposit, totaling over \$670,000, all from known or suspected victims. The FBI interviewed nine additional victims that deposited money into the Dragon Auto bank accounts, all indicating that money transfers were the result of a tech support scam.

26. Based on the fraudulent activity described above, I reviewed the Commonwealth of Virginia SCC records to identify additional businesses located at 7630 Little River Turnpike. This review identified several fictitious businesses, including:

- a. M&M Popular Package Food Inc. (EIN: 93-1572743, registered agent X.W.)
- b. LL Wang Food Trading Inc. (EIN: 93-1571607, registered agent L.W.)
- c. Crysal Accessories Inc. (EIN: 93-1916200, registered agent H.C.)

The investigation has identified each of the businesses referenced above was also associated with the residential address of 1515 Richmond Hwy. LocalWorks and Crystal Square Apartments had no records of the above individuals or entities being associated with their properties.

27. On April 25, 2024, I interviewed X.W., an identity theft victim, whose information was used to incorporate M&M Popular Package Food Inc. X.W. indicated that his identity appeared to have been stolen in the summer of 2023. X.W. filed a police report on July 10, 2023 related to the identity theft. I have compared the photographs of the individual depicted in the M&M Popular Package Food Inc. bank surveillance footage to the individual I interviewed in April 2024 and do not believe the person depicted in the surveillance footage is X.W. I have compared the surveillance footage to known pictures of LIANG. Based on my review, I believe the person depicted in the surveillance footage (purporting to be X.W.) to be LIANG.

28. Upon reviewing various bank records, IRS's Mod IEIN records, Postal Service Records and the Virginia State Corporation Commission ("SCC") records, numerous businesses have been identified as being operated by LIANG, LI, and/or other co-conspirators in furtherance of the scheme. The businesses identified include, but are not limited to, the following (collectively the "Fictitious Virginia Business Entities"):

- a. Dragon Auto Parts Inc
- b. M&M Popular Package Food Inc
- c. LL Wang Food Trading Inc
- d. Crystal Accessories Inc
- e. V&L Good Food Wholesale Inc
- f. Dug Duy Food Trading Inc
- g. Coco Love Nail Art Wholesale Inc
- h. Kim Fashionable Clothing Inc
- i. Leslie Cell Phone Accessories
- j. Roger Trucking Service
- k. Above and Beyond Heating Corp
- l. Kunblo Spring City Inc
- m. SZ Façade Management Inc
- n. Universe CCK Computer Inc
- o. Dragon Façade Management
- p. Hong & Yun Clothing Inc
- q. LMH Computer Service Inc

- r. Carson Truck Service Inc
- s. Phenix Beauty Supplies Inc
- t. Chia Supplies Co Limited
- u. Lena Castle Inc
- v. S&W Façade Management Inc
- w. Pure Life HL Inc
- x. BHB Products Trading Inc
- y. LT Restaurant Supplies Inc
- z. SSW Investment Inc
- aa. UJS Equipment Inc
- bb. Amcor Plus One Wholesale Inc

29. On April 30, 2024, a federal search warrant (1-24-SW-304) was issued by the Honorable Magistrate Judge Ivan D. Davis in the Eastern District of Virginia for three devices in LIANG's hotel room. On the cell phone associated with a phone number connected to LIANG, I reviewed WeChat communications between LIANG and coconspirators. The WeChat communications included identification documents, Virginia SCC incorporation documents, utility bills, and financial information associated with many of the Fictitious Virginia Business Entities.

The Fictitious Virginia Business Entity Bank Accounts

30. To date, I have reviewed over 100 bank accounts associated with the Fictitious Virginia Business Entities, including the **SUBJECT ACCOUNTS**. Review of the bank account activity associated with the Fictitious Virginia Business Entities did not identify business income

or business expenses. Rather, the bank accounts have nearly no activity other than the receipt of victim funds and the transfer of those funds to other bank accounts or the cash withdrawal of funds.

31. The bank accounts, including the **SUBJECT ACCOUNTS**, were often only kept open for a couple of months before being closed by the banks. Accordingly, each Fictitious Virginia Business Entity often held bank accounts at multiple financial institutions. For example, as discussed above, bank accounts associated with Dragon Auto Parts were opened at PNC, Truist, TD Bank, Citibank, Wells Fargo, United Bank, and Capital One. All seven of the Dragon Auto Parts bank accounts were opened between June 21, 2023 and September 5, 2023 and all the accounts had been closed by November 2023.

32. Based on my review of bank surveillance footage, an individual resembling LIANG was depicted conducting financial transactions associated with at least eight different entities, including Dragon Auto Parts Inc, LL Wang Food Trading Inc, Kunblo Spring City Inc, Crystal Accessories, M&M Popular Package Food Inc, SZ Façade Management Inc, Roger Trucking Service Inc, and Kim Fashionable Clothing Inc. None of the bank account signature cards indicate that LIANG is an authorized signor. The bank account signatories associated with each of the Fictitious Virginia Business Entities are different.

33. Review of WeChat communications on LIANG's device revealed that the coconspirators exchanged numerous credit reports, driver's license photographs, social security numbers, addresses, and date of birth for the individuals listed as registered agents and signatories for the Fictitious Virginia Business Entities. Review of the WeChat communications on LIANG's device also revealed the exchange of bank account information, such as passwords

and account numbers, associated with many of the Fictitious Virginia Business Entities and bank accounts linked to other suspected fictitious businesses. I believe this was done to enable multiple people to have access to the bank accounts in order to conduct and review financial transactions. For example, on November 16, 2023, an individual with the WeChat username ‘Customs’⁴ asked LIANG and coconspirators to “prepare the specialized account just for receiving the scam chat, and then get a few corporate entities to receive the cashier’s checks.” ‘Customs’ further stated, “the customer is rushing me daily to send accounts.” A few hours later, a coconspirator⁵ then sent the following account information:

CITI BANK TOKEN
Business name BHB PRODUCTS TRADING INC
Business code 700000000645147
User id 463
Password Cal210038@

Business Checking
• *Name: BHB PRODUCTS TRADING INC*
• *Address of company 6801 Richmond HWY STE 201 Alexandria VA 22306*
• *Account#: 9250977018*
• *Fedwire ABA for wires: 254070116*
Address of bank :3241 14th st nw Washington DC 20010
ONLINE BANK hb1980bao
PASSWORD :Cal210038@

Review of the WeChat conversations further indicated that ‘Customs,’ and other conspirators, accessed and attempted to access the bank accounts using the account information provided.

⁴ “Customs,” associated with WeChat ID wxid_5z4lkp1etp2212, was observed communicating with LIANG and other coconspirators on when to expect victim deposits, which accounts to direct victim funds be deposited into, and where to send the victim funds once received.

⁵ WeChat ID wxid_qmpg4rcyzx4a12, username “Breaking Waves.”

34. Review of the bank account opening documents indicated that a Dominion Energy utility bill associated with account number 6623958664, meter number 4825442, was often submitted for address verification. Records from Dominion Energy indicated that the meter number did not exist and that the account number was associated with an unrelated government entity. In reviewing the WeChat conversations, I identified numerous instances in which fictitious Dominion Energy utility bills were shared for different entity names, registered agent names, and addresses. On August 7, 2023, LIANG asks a coconspirator⁶ to update the utility bill. The coconspirator then sends the following image, depicting the areas of the utility bill that were changed:

⁶ WeChat ID a25658977, username “lulu.”

SOVIEW ADORN...T DESIGN INC.pdf

Dominion Energy

Billing and Payment Summary

Jun 05, 2023	Customer Bill
MC POPULAR SNACK INC	8731 PLANTATION LN MANASSAS VA 20110-1680
Account # 662395864 Due Date: Jul 10, 2023	
Total Amount Due: \$ 290.11	

To avoid a Late Payment Charge of 1.5% please pay by Jul 10, 2023.

Previous Amount Due: \$ 290.70
Payments as of Jun 05: \$ 290.70CR

For service emergencies and power outages please call 1-866-DCM4HELP (1-866-369-4257). Visit us at www.dominionenergy.com.

Meter and Usage

Current Billing Days: 32		Mo	Yr	kWh
Billable Usage	Schedule GS-2	Jun	22	9620
Total kWh	05-02-06-03	Jul	22	7424
Demand	43008	Aug	22	4140
	105.0	Sep	22	2240
		Oct	22	4544
		Nov	22	6230
		Dec	22	6672
		Jan	23	7248
		Feb	23	6600
		Mar	23	8400
		Apr	23	0320
		May	23	2640
		June	23	3008
Meter:	0004625442			
Current Reading	43008			
Previous Reading	10592			
Total kWh	43008			
Current Reading	55			
Demand	105.60			
Multiplier:	192			

Measured Usage

Mo	Yr	kWh
Jun	22	9620
Jul	22	7424
Aug	22	4140
Sep	22	2240
Oct	22	4544
Nov	22	6230
Dec	22	6672
Jan	23	7248
Feb	23	6600
Mar	23	8400
Apr	23	0320
May	23	2640
June	23	3008

Usage History

Explanation of Bill Detail

Customer Service	1-866-591-0157
Previous Balance	290.70
Payment Received	290.70CR
Balance Forward	0.00
Non-Residential Service (Schedule GS-2) - 05-02-06-03	
Distribution Service Charge	1.22
Distribution Service kWh	0.22
Distr Serv Demand Charge	56.49
49 Applicable Demand Riders	1.17
Electricity Supply Svc (ESS)	
Electricity Supply kWh	242.11
Electricity Supply Demand Charge	24.11
Transmission Demand Chg	20.76
Fuel	161.21
All Other Applicable ESS Riders	18.18
Sales and Use Surcharge	9.78
Base Rate Case Credit	23.61 CR
Total Current Charges	290.11

Total Account Balance **290.11**

View payment options, request service changes and enroll in eBill at www.dominionenergy.com; search: Manage Your Account.

Important Customer Information from Dominion Energy Virginia

Your bill includes a credit for electric service between January 1, 2022 and March 31, 2023. This credit is being provided to pass on 100% of tax savings Dominion Energy Virginia gained through a federal tax reform in 2022. For more details, visit [DominionEnergy.com/verates](http://www.dominionenergy.com/verates).

Please record your account number on your check and mail payment to: Dominion Energy Virginia, PO Box 26543, Richmond, Va. 23290-0001.

Mailed on Jun 06, 2023

Please detach and return this payment coupon with your check made payable to Dominion Energy Virginia. Please see reverse side for mailing address change instructions.

Payment Coupon

Bill Date Jun 05 23	Please Pay by 07/10	Amount Enclosed
\$ 290.11		

MC POPULAR SNACK INC 00073-0

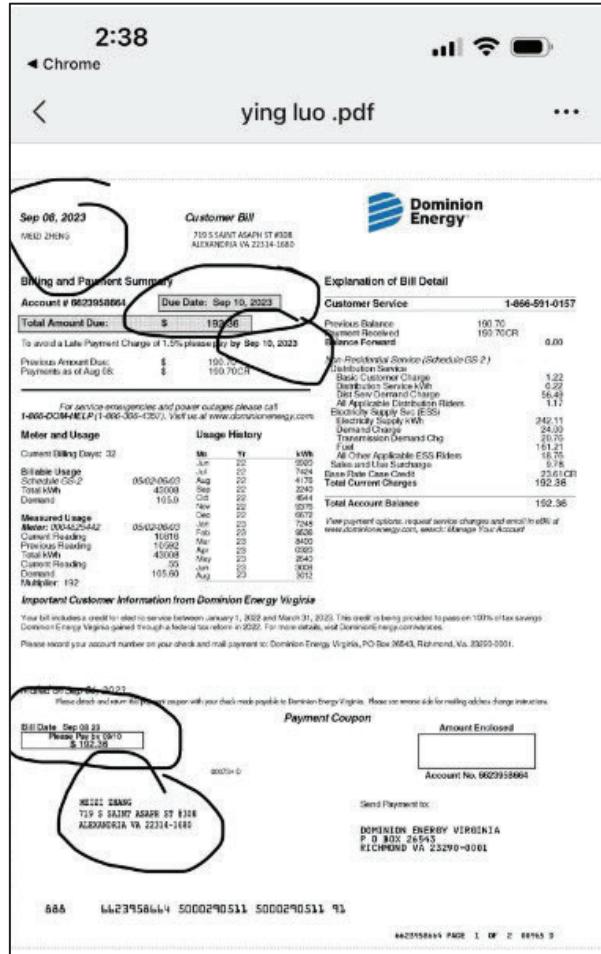
MC POPULAR SNACK INC
8731 PLANTATION LN
MANASSAS VA 20110-1680

Send Payment to:
DOMINION ENERGY VIRGINIA
P O BOX 26543
RICHMOND VA 23290-0001

3 2

888 662395864 5000290511 5000290511 91

35. Similarly, on January 21, 2024, ‘Customs’ informed coconspirators that they were trying to create a new Kraken account and they needed to provide proof of address in Virginia. ‘Breaking Waves’ responded, “It’s all fake” and provided the following image, depicting the areas of the utility bill that needed to be changed:



36. The signatory cards associated with the account opening documents for the Fictitious Virginia Business Entities often indicate fictitious business purposes for the accounts. At times, incoming wire memos from victims reference fictitious business purposes, such as the purchase of a home, goods, or to support a friend's new business. Conspirators would often tell victims what to put in the wire memo line when sending the wire. I interviewed W.B., a 70-year-old residing in Two Rivers, Wisconsin, who told the bank that he sent \$18,099 to Dragon Auto Parts in order to purchase a truck, even though there was no truck.

37. Instead, the true source of the funds derived from tech support and other elder

fraud scams. On December 10, 2023, ‘Customs’ sent the following WeChat messages, indicating that the source of funds for these accounts relates to scams:

CITI BANK (Thuy)
Business name : LT RESTAURANT SUPPLIES INC

Business Checking

- *Name: LT RESTAURANT SUPPLIES INC*
- *Address of company : 105 ORONOCO ST STE 300, Alexandria VA 22314*
- *Account#: 9250977565*
- *Fedwire ABA for wires: 254070116*

Swift code: CITIUS33

Address of bank : 1400 G St NW, Washington DC, 20005

CITI BANK

Business name BHB PRODUCTS TRADING INC

Business Checking

- *Name: BHB PRODUCTS TRADING INC*
- *Address of company 6801 Richmond HWY STE 201 Alexandria VA 22306*
- *Account#: 9250977018*
- *Fedwire ABA for wires: 254070116*

Swift code: CITIUS33

Address of bank : 3241 14th st nw Washington DC 20010

(management range): if customers demand remarks/notes then remark to purchase from our side cellphone and computer parts

Swift code if funds coming from other countries please use Swift code: CITIUS33
(incoming funds range) : 10k-500k

there are no incoming funds amount restrictions

holiday incoming funds account

these two are to receive the small amounts from chat scams, referring to the single amounts of less than one hundred thousand

38. An excerpt of a January 4, 2024 conversation between LIANG and a

coconspirator⁷ is below:

LIANG: I have quite a few of my fake customers doing more than a million

Busy: what's the reason

Busy: is it clean funding or what

LIANG: all are scams

39. Based on my training and experience and the context of the WeChat conversation, I believe that LIANG is referencing the Fictitious Virginia Business Entities with the phrase ‘fake customers.’ Furthermore, I believe that the phrase ‘doing more than a million’ references the amount of deposits LIANG is able to receive before the bank closes the account. Notably, LIANG confirms that the bank account deposits relate to scam proceeds.

40. Review of the WeChat communications on LIANG’s device also included instructions on where to send the funds deposited into the bank accounts associated with the Fictitious Virginia Business Entities. For example, on February 21, 2024, ‘Customs’ sends the bank account information for Kelsea Limited and states “Only used for the refund of Account Name: Lena Castle Inc.” ‘Customs’ provides numerous accounts as withdrawal accounts for the scam proceeds, including: AUS Merchant Services, Kelsea Limited, and Tiger Fly Co. Notably, records from JP Morgan Chase indicated that even though the outgoing wires to Citibank accounts associated with Tiger Fly Co and Kelsea Limited appear to be credited to U.S.-based financial institutions, the true beneficiary is AUS Merchant Services, which is associated with Alipay.⁸ Based on my training and experience, I believe that these outgoing wires are a method to move the victim funds from the United States back to China.

7 WeChat ID, username “busy.”

8 <https://global.alipay.com/docs/ac/Platform/qd977g#alipay-us-inc>.

The Subject Accounts

41. The government has employed the lowest intermediate balance rule (“LIBR”) in analyzing the **SUBJECT ACCOUNTS**, meaning the government determined which funds in the respective accounts constitute, or are traceable to, the proceeds of the mail and wire fraud scheme, and which funds are “other funds,” *i.e.*, funds not traceable to the mail and wire fraud scheme. LIBR is a method in which the government assumes the “other funds” in a bank account are spent before any funds in the account that constitute or are traceable to the mail and wire fraud scheme. This analysis is strictly based on the categorization of funds and not on the time of deposit; in these analyses, funds derived from a fraud scheme could stay in a bank account for years if the bank account was continually replenished with “other funds” for substantial periods of time.

SUBJECT ACCOUNT 1

42. On or around July 2, 2023, S&W Façade Management Inc was registered with the Virginia SCC. On or around August 16, 2023, Citibank account number 9250974043 in the name of S&W Façade Management Inc was opened (“**SUBJECT ACCOUNT 1**”). Prior to September 5, 2023, **SUBJECT ACCOUNT 1** had a balance of \$100. On September 5, 2023, **SUBJECT ACCOUNT 1** received one deposit of \$349,957 from K.A., a resident of Keller, Texas. **SUBJECT ACCOUNT 1** received no additional deposits. On November 21, 2023, **SUBJECT ACCOUNT 1** was closed and Citibank moved \$349,957 to an internal Citibank account.

43. K.A. was interviewed by the FBI and submitted an IC3 complaint indicating that she was the victim of a scam and initiated the wire transaction under fraudulent pretenses. As of

August 21, 2024, Citibank is holding approximately \$349,957 in an internal Citibank account associated with **SUBJECT ACCOUNT 1**. The funds remaining in **SUBJECT ACCOUNT 1** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 2

44. On or around August 10, 2023, Carson Truck Service Inc was registered with the Virginia SCC. On or around September 6, 2023, Citibank account number 9250974523 in the name of Carson Truck Service Inc was opened (“**SUBJECT ACCOUNT 2**”). **SUBJECT ACCOUNT 2** received the following deposits, as detailed below:

- September 6, 2023: \$34,150 from J.K, an 80-year-old residing in Minneapolis, Minnesota
- September 8, 2023: \$8,000 from D.A., a 75-year-old residing in Taylorsville, Utah
- September 8, 2023: \$10,000 from J.H.
- September 8, 2023: \$73,250 from M.H., a 55-year-old residing in Holly, Michigan

45. On September 8, 2023, **SUBJECT ACCOUNT 2** wired \$93,998 to Tian Catering Corp. On October 5, 2023, **SUBJECT ACCOUNT 2** received a deposit of \$93,998 from Tian Catering Corp. The deposit appears to represent the return of the September 8, 2023 transfer for the same amount. No additional deposits occurred in **SUBJECT ACCOUNT 2**.

46. J.K. filed an IC3 complaint indicating that they were the victim of a tech support scam. On October 2, 2023, Dort Financial Credit Union sent a Hold Harmless and Indemnity Agreement (“Hold Harmless”) related to the wire transfer from M.H. Based on my training and experience, I know that Hold Harmless letters are often sent after a victim has informed their bank that they were the victim of a fraud scheme and is attempting to recover their funds. On August 22, 2024, D.A. confirmed that their \$8,000 wire transfer to **SUBJECT ACCOUNT 2**

was the result of a scam. On August 24, 2024, I interviewed M.H. who indicated that they were the victim of a tech support scam and that they had also filed a police report with their local police department. On or around November 2, 2023, Citibank returned \$10,000 to J.H., who informed Citibank that the wire transfer was fraudulent.

47. As of August 21, 2024, Citibank is holding approximately \$83,983 in an internal Citibank account associated with **SUBJECT ACCOUNT 2**. The funds remaining in **SUBJECT ACCOUNT 2** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 3

48. On or around August 2, 2023, Pure Life HL Inc was registered with the Virginia SCC. The registered agent is listed as Hui Lin. On June 7, 2024, Hui Lin submitted an identity theft application related to the Pure Life HL Inc account opened at Truist. Further, Hui Lin's driver's license number, social security number, date of birth, and address were located in the review of LIANG's WeChat conversations.

49. On or around September 25, 2023, Citibank account number 9250975619 in the name of Pure Life HL Inc was opened ("SUBJECT ACCOUNT 3"). On September 29, 2023, LIANG sent the following WeChat message:

2. *CITI(HUI-LIN大)*
 - *Online Banking*
 - *username: lin1973hui*
 - *password: Cal210038@*
 - *Name: Pure Life HL INC*
 - *Address of Company: 8731 Plantation Ln Manassas, VA 20110*
 - *Account#:9250975619*
 - *Wire Routing#: 254070116*
 - *Address of Bank: 7633 New Hampshire ave Takoma Park, MD 20912*

50. Between October 3, 2023 and October 4, 2023, **SUBJECT ACCOUNT 3**

received four deposits, as detailed below:

- October 3, 2023: \$16,500 from P.S., holding a bank account at Harvesters Federal Credit Union (“FCU”)
- October 3, 2023: \$23,925 from R.S., a 74-year-old residing in South Padre Island, Texas
- October 4, 2024: \$33,500 from One Source FCU
- October 4, 2024: \$35,000 from J.S., an 81-year-old residing in Cleveland, Ohio

51. There were no additional deposits into **SUBJECT ACCOUNT 3**. On October 10, 2023, R.S. submitted an IC3 complaint stating that they were the victim of a tech support scam. On October 10, 2023, a Hold Harmless letter was submitted on behalf of J.S. and her funds were returned. I was unable to locate P.S.; however, Harvesters FCU appears to service five counties in Florida. One Source FCU is located in El Paso, Texas and Las Cruces, New Mexico. Based on my training and experience, and the investigation conducted to date, I believe that the wires from P.S. and One Source FCU were the result of a tech support or similar elder fraud scam.

52. As of August 21, 2024, Citibank is holding approximately \$58,096 in an internal Citibank account associated with **SUBJECT ACCOUNT 3**. I have probable cause to believe that the funds remaining in **SUBJECT ACCOUNT 3** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 4

53. On or around October 19, 2023, BHB Products Trading Inc was registered with the Virginia SCC. On or around October 25, 2023, Citibank account number 9250977018 in the name of BHB Products Trading Inc was opened (“**SUBJECT ACCOUNT 4**”).

54. As discussed in paragraph 37 above, the bank account and login information for **SUBJECT ACCOUNT 4** was shared in WeChat conversations involving LIANG. The WeChat messages indicated that the source of funds for **SUBJECT ACCOUNT 4** was “chat scams.”

55. Prior to December 8, 2023, **SUBJECT ACCOUNT 4** had a balance of \$7,444.84. On December 8, 2023, **SUBJECT ACCOUNT 4** received five deposits, as detailed below:

- December 8, 2023: \$1,000 from L.R., a 64-year-old residing in West Jefferson, North Carolina
- December 8, 2023: \$1,000 from Z.P.K., a 72-year-old residing in Independence, Virginia
- December 8, 2023: \$10,000 from Z.B., holding a bank account at Pinnacle Bank
- December 8, 2023: \$40,000 from P.B., holding a bank account at Wells Fargo
- December 8, 2023: \$50,500 from B.H., a 60-year-old residing in Sugar Land, Texas

56. No additional deposits occurred in **SUBJECT ACCOUNT 4**. A Hold Harmless letter was submitted on behalf of P.B. and her funds were subsequently returned. On August 23, 2024, Z.P.K. confirmed that the \$1,000 deposit related to an elder fraud scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from L.R., Z.B., and B.H. were also the result of a tech support or similar elder fraud scam.

57. As of August 21, 2024, Citibank is holding approximately \$54,127.44 in an internal Citibank account associated with **SUBJECT ACCOUNT 4**. I have probable cause to believe that the funds remaining in **SUBJECT ACCOUNT 4** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 5

58. On or around June 16, 2023, Leslie Cell Phone Accessories Inc was registered

with the Virginia SCC. On or around July 3, 2023, Citibank bank account number 9250972814 in the name of Leslie Cell Phone Accessories Inc was opened (“**SUBJECT ACCOUNT 5**”). Between July 3, 2023 and July 6, 2023, **SUBJECT ACCOUNT 5** received \$121,776 in deposits, as detailed below:

- July 3, 2023: \$50,000 from D.B., a 59-year-old residing in Las Vegas, Nevada
- July 5, 2023: \$19,500 from B.M., a 74-year-old residing in Montrose, South Dakota
- July 6, 2023: \$9,000 from R.S., an 86-year-old residing in Harlingen, Texas
- July 6, 2023: \$20,000 from X.F., related to the return of a previously attempted withdraw
- July 6, 2023: \$23,276, from V.P., a 79-year-old residing in Lake Jackson, Texas

59. **SUBJECT ACCOUNT 5** received \$200.30 in additional deposits. The wire from B.M. was returned associated with a Hold Harmless letter. V.P. filed an IC3 complaint indicating that she was the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from D.B. and R.S. were also the result of a tech support or similar elder fraud scam.

60. As of August 21, 2024, Citibank is holding approximately \$49,459.30 in an internal Citibank account associated with **SUBJECT ACCOUNT 5**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 5** are victim funds, and the remaining funds in **SUBJECT ACCOUNT 5** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 6

61. On or around October 26, 2023, LT Restaurant Supplies Inc was registered with

the Virginia SCC. On or around November 17, 2023, Citibank bank account number 9250977565 in the name of LT Restaurant Supplies Inc was opened (“**SUBJECT ACCOUNT 6**”). On November 29, 2023, LIANG sent the bank account information associated with **SUBJECT ACCOUNT 6** in a WeChat conversation with ‘Customs’ and others. Throughout December, ‘Customs’ asked for videos of **SUBJECT ACCOUNT 6** to review account deposits and withdrawals.

62. Between November 17, 2023 and December 7, 2023, **SUBJECT ACCOUNT 6** received 15 deposits totaling \$321,185. Three of the deposits, totaling \$102,700, were returned to senders due to Hold Harmless letters being sent. One of the individuals associated with a Hold Harmless letter also submitted an IC3 complaint indicating that they were the victim of an elder fraud scam. Other deposits into **SUBJECT ACCOUNT 6** included the following:

- December 7, 2023: \$3,000 from B.P., a 79-year-old residing in Little Neck, New York
- December 7, 2023: \$101,000 from W.R., a 73-year-old residing in Kihei, Hawaii

63. The son of B.P. filed an IC3 complaint indicating that their father was the victim of an elder fraud scam, resulting in fraudulent wire transfers including the deposit into **SUBJECT ACCOUNT 6**. Based on my training and experience, and the investigation conducted to date, I believe that the wire from W.R. was also the result of a tech support or similar elder fraud scam.

64. As of August 21, 2024, Citibank is holding approximately \$49,412.53 in an internal Citibank account associated with **SUBJECT ACCOUNT 6**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 6** are victim funds and the remaining funds in **SUBJECT ACCOUNT 6** constitute the proceeds of the mail and wire

fraud scheme.

SUBJECT ACCOUNT 7

65. On or around October 17, 2023, Phenix Beauty Supplies Inc was registered with the Virginia SCC. On or around October 20, 2023, Citibank bank account number 9111716029 in the name of Phenix Beauty Supplies Inc was opened (“**SUBJECT ACCOUNT 7**”). On November 17, 2023, ‘Customs’ sent the bank account information associated with **SUBJECT ACCOUNT 7** in a WeChat group conversation and asked for a video of the account in order to review the account transactions.

66. Prior to November 29, 2023, the balance of **SUBJECT ACCOUNT 7** was \$26,392.12. **SUBJECT ACCOUNT 7** received the following additional deposits:

- November 29, 2024: \$4,400 from A.J.
- November 29, 2023: \$42,562.95 from N.F., a 34-year-old residing in Croton On Hudson, New York
- November 29, 2023 and November 30, 2023: \$20,000 from K.J.
- December 6, 2024: \$14,000 from D.A., a 42-year-old residing in Stow, Massachusetts

67. D.A. and N.F. filed IC3 reports indicating that their wire transactions related to fraudulent investment scams.

68. As of August 23, 2024, Citibank is holding approximately \$27,503.76 in an internal Citibank account associated with **SUBJECT ACCOUNT 7**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 7** are victim funds and the remaining funds in **SUBJECT ACCOUNT 7** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 8

69. On or around March 31, 2023, Kim Fashionable Clothing Inc was registered with the Virginia SCC. On or around June 6, 2023, Citibank bank account number 9250969228 in the name of Kim Fashionable Clothing Inc was opened (“**SUBJECT ACCOUNT 8**”). Prior to June 12, 2023, **SUBJECT ACCOUNT 8** had a balance of \$5,045. Between June 12, 2023 and June 14, 2023, **SUBJECT ACCOUNT 8** received seven deposits, totaling \$170,400. Two of the deposits, totaling \$99,400, were subsequently returned associated with Hold Harmless letters. The remaining deposits were comprised of the following:

- June 13, 2023: \$2,000 from G.B., holding a bank account at Wells Fargo
- June 13, 2023: \$5,000 from M.B., a 62-year-old residing in Manor, Texas
- June 13, 2023: \$44,000 from S.R., an 83-year-old residing in Renton, Washington
- June 14, 2023: \$5,000 and \$15,000 deposits from T.O.K.M., holding a bank account at Al Hali Bank of Kuwait

70. **SUBJECT ACCOUNT 8** received no additional deposits. S.R. filed an IC3 complaint indicating that she was the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from G.B., M.B., and T.O.K.M. were also the result of a tech support or other elder fraud scam.

71. As of August 21, 2024, Citibank is holding approximately \$20,948.82 in an internal Citibank account associated with **SUBJECT ACCOUNT 8**. I have probable cause to believe that the funds held in **SUBJECT ACCOUNT 8** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 9

72. On or around August 28, 2023, SSW Investment Inc was registered with the Virginia SCC. Shine Wang was listed as the registered agent. On or around August 30, 2023, TD Bank account number 4441079377 in the name of SSW Investment Inc was opened (“**SUBJECT ACCOUNT 9**”).

73. On November 13, 2023, the bank account information associated with SSW Investment Inc’s Truist bank account was shared by a coconspirator via WeChat. Included in the message was the online banking login information, phone number associated with the account, social security number associated with the registered agent and full driver’s license number. Shine Wang’s TransUnion and Equifax credit reports were also shared in WeChat conversations.

74. Prior to September 15, 2023, the balance of **SUBJECT ACCOUNT 9** was \$315.62. Between September 15, 2023 and September 18, 2023, **SUBJECT ACCOUNT 9** received three deposits, totaling \$191,855, as detailed below:

- September 15, 2023: \$47,400 from A.N., via cashier’s check payable to Mark Wilson SSW
- September 15, 2023: \$44,500 from A.G., a 73-year-old residing in Central, South Carolina
- September 18, 2023: \$99,955 from J.S., a 73-year-old residing in Bloomington, Indiana

75. **SUBJECT ACCOUNT 9** received no additional deposits. A.G. filed an IC3 indicating that they were the victim of a tech support scam. Further, review of IC3 indicated several reports of a ‘Mark Wilson’ purporting to be a representative of Microsoft or another technology company associated with tech support scams. Based on my training and experience,

and the investigation conducted to date, I believe that the funds from A.N. and J.S. were also the result of a tech support or other elder fraud scam.

76. As of August 21, 2024, TD Bank indicated funds totaling up to approximately \$148,906.88 were being held in an internal TD Bank account associated with **SUBJECT ACCOUNT 9**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 9** are victim funds, and the remaining funds in **SUBJECT ACCOUNT 9** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 10

77. On or around April 27, 2023, Above and Beyond Heating Corp was registered with the Virginia SCC. On or around May 22, 2023, TD Bank account number 4408454356 in the name of Above and Beyond Heating Corp was opened ("**SUBJECT ACCOUNT 10**"). Prior to June 14, 2023, **SUBJECT ACCOUNT 10** had a balance of \$14.81. Between June 14, 2023 and June 15, 2023, **SUBJECT ACCOUNT 10** received three deposits, totaling \$82,500, as detailed below:

- June 14, 2023: \$45,000 from K.S., a 91-year-old residing in Folsom, California
- June 14, 2023: \$30,000 from J.V., an 88-year-old residing in Dickinson, North Dakota
- June 15, 2023: \$7,500 from A.B., a 61-year-old residing in Brooklyn, New York

78. **SUBJECT ACCOUNT 10** received an additional \$2.42 in interest payments. K.S. reported to their local police department that they were the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from J.V. and A.B. were also the result of a tech support or other elder fraud scam.

79. As of August 21, 2024, TD Bank indicated funds totaling up to approximately

\$82,472.23 were being held in an internal TD Bank account associated with **SUBJECT ACCOUNT 10**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 10** are victim funds, and the remaining funds in **SUBJECT ACCOUNT 10** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 11

80. On or around March 31, 2023, Kim Fashionable Clothing Inc was registered with the Virginia SCC. On or around April 5, 2023, TD Bank account number 4408376617 in the name of Kim Fashionable Clothing Inc was opened (“**SUBJECT ACCOUNT 11**”). Prior to June 29, 2023, the balance in **SUBJECT ACCOUNT 11** was \$591.80. **SUBJECT ACCOUNT 11** received four deposits on June 29, 2023, totaling \$102,833, as detailed below:

- June 29, 2023: \$35,000 from S.M., a 72-year-old residing in Carol Stream, Illinois
- June 29, 2023: \$30,333 from A.D., a 67-year-old residing in Portland, Oregon
- June 29, 2023: \$29,500 from Tie & Timber Technologies
- June 29, 2023: \$8,000 from K.S., a 68-year-old residing in Corvallis, Oregon

81. **SUBJECT ACCOUNT 11** received no additional deposits. Tie & Timber Technologies subsequently submitted an IC3 complaint indicating that the wire transfer was the result of a scam. TD Bank later returned the funds to Tie & Timber Technologies. A.D. also submitted an IC3 complaint indicating that they were the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from S.M. And K.S. were also the result of a tech support or other elder fraud scam.

82. As discussed above, LIANG was observed on bank surveillance footage conducting financial transactions associated with a Bank of America account in the name of Kim

Fashionable Clothing Inc.

83. As of August 21, 2024, TD Bank indicated funds totaling up to approximately \$73,049.30 were being held in an internal TD Bank account associated with **SUBJECT ACCOUNT 11**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 11** are victim funds, and the remaining funds in **SUBJECT ACCOUNT 11** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 12

84. On or around November 15, 2023, UJS Equipment Inc was registered with the Virginia SCC. On or around December 6, 2023, TD Bank account number 4441223776 in the name of UJS Equipment Inc was opened (“**SUBJECT ACCOUNT 12**”).

85. On December 13, 2023, ‘Customs’ sent the following WeChat messages:

*Bank Name:TD BANK
Account Name: UJS Equipment INC
Account number:4441223776
Address of the bank:1750 North Hampton Ave Reston,VA 20194
Company/Personal Address:6801 Richmond Hwy suite 201 Alexandria VA 22306
FEDWIRE ABA FOR WIRES:031101266*

I want a video from this account

On the same day, LIANG sent a video logging into **SUBJECT ACCOUNT 12**, showing a balance of \$100.02.

86. Prior to December 14, 2023, the balance of **SUBJECT ACCOUNT 12** was \$100.02. On December 14, 2023, **SUBJECT ACCOUNT 12** received \$28,400 from an 84-year-old residing in Pelham, New Hampshire, which I believe was the result of a tech support or other elder fraud scam. There were no other deposits into the account.

87. As of August 21, 2024, TD Bank indicated funds totaling up to approximately

\$28,485.02 were being held in an internal TD Bank account associated with **SUBJECT ACCOUNT 12**. I have probable cause to believe that up to \$28,400 held related to **SUBJECT ACCOUNT 12** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 13

88. On or around March 22, 2023, LMH Computer Service Inc was registered with the Virginia SCC. On or around April 18, 2023, TD Bank account number 4408354192 in the name of LMH Computer Service Inc was opened (“**SUBJECT ACCOUNT 13**”). **SUBJECT ACCOUNT 13** received the following four wires:

- April 18, 2023; \$38,000 from F.C., a 74-year-old residing in Burnet, Texas
- April 18, 2023: \$9,530 from W.M., a 77-year-old residing in Pittsburgh, Pennsylvania
- April 20, 2023: \$25,000 from P.S., an 80-year-old residing in Oldsmar, Florida
- April 20, 2023: \$19,800 from W.B., a 72-year-old residing in Mesa, Arizona

89. **SUBJECT ACCOUNT 13** received \$85 in additional deposits. W.B. reported to her local police department that she was the victim of a tech support scam. The wires from W.B. and W.M. were subsequently returned. Based on my training and experience, and the investigation conducted to date, I believe that the wires from F.C. and P.S. were also the result of a tech support or other elder fraud scam.

90. On April 20, 2023, a cashier’s check for \$30,000 payable to Staring LLC was purchased. Staring LLC is an entity controlled by LI and purportedly was involved in the “diamond trade.” However, a review of Staring LLC’s bank accounts indicated that the accounts received funds from coconspirator bank accounts and then quickly wired the money to other domestic and international bank accounts.

91. As of August 21, 2024, TD Bank indicated funds totaling up to approximately \$22,046 were being held in an internal TD Bank account associated with **SUBJECT ACCOUNT 13**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 13** are victim funds, and the remaining funds in **SUBJECT ACCOUNT 13** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 14

92. On or around July 13, 2023, Pure Life HL Inc was registered with the Virginia SCC. On or around September 13, 2023, JP Morgan Chase bank account number 550635711 in the name of Pure Life HL Inc was opened (“**SUBJECT ACCOUNT 14**”). On October 11, 2023, the balance of **SUBJECT ACCOUNT 14** was \$3,850. On October 12, 2023, **SUBJECT ACCOUNT 14** received three wires, totaling \$160,054.23, as detailed below:

- October 12, 2023: \$14,800 from G.O., a 76-year-old residing in Lodi, California
- October 12, 2023: \$97,254.23 from R.M., a 74-year-old residing in Fort Lauderdale, Florida
- October 12, 2023: \$48,000 from L.B., an 82-year-old residing in Dana Point, California

93. **SUBJECT ACCOUNT 14** received no other deposits. On August 20, 2024, G.O. stated that this wire was the result of a tech support scam. On August 20, 2024, L.B. stated that this wire was the result of a tech support scam. J P Morgan Chase later returned L.B.’s funds. R.M. filed an IC3 complaint stating that they were the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wire from R.M. was also the result of a tech support or other elder fraud scam.

94. As of August 21, 2024, JP Morgan Chase is holding approximately \$90,000 in an

internal JP Morgan Chase account associated with **SUBJECT ACCOUNT 14**. I have probable cause to believe funds in **SUBJECT ACCOUNT 14** are victim funds and constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 15

95. On or around December 19, 2023, Chia Supplies Co Limited was registered with the Virginia SCC. The registered agent is listed as Chia-yu Dennis Liu. On December 7, 2023, LIANG, via WeChat, shared a picture of Liu's Texas driver's license, Liu's date of birth, and Liu's social security number. LIANG requested that a coconspirator run a credit report for Liu. Based on the investigation to date, this activity is consistent with LIANG using another individuals identifying information in order to register a fictitious business open and open bank accounts to receive victim funds.

96. On or around January 4, 2024, JP Morgan Chase bank account number 575850907 in the name of Chia Supplies Co Limited was opened ("SUBJECT ACCOUNT 15"). On January 4, 2024, 'Breaking Waves,' a co-conspirator sent the following WeChat message:

*Bank Name:CHASE BANK
Account Name:chia supplies co limited
Routing number:044000037
Account number:575850907
Address of the bank:270 Park Ave New York NY 10017
Company address:6801 Richmond HWY STE 201 Alexandria VA 22306
FEDWIRE ABA FOR WIRES:021000021
CHASE SWIFT CODE:CHASUS33
ONLINE BANK: liu1970chia
PASS WORD:Piao1097!*

'Customs' then told 'Breaking Waves' that the company name looks like it is from Hong Kong and it's best to use INC or LLC to end company names.

97. Prior to January 18, 2024, **SUBJECT ACCOUNT 15** had a balance of \$44,318.

SUBJECT ACCOUNT 15 received an additional \$65,204 in deposits, including:

- January 18, 2024: \$52,404 from M.A., an 85-year-old residing in Spokane, Washington
- January 18, 2024: \$5,500 from C.S., a 68-year-old residing in Knotts Island, North Carolina
- January 18, 2024: \$800 Zelle from M.C.
- January 22, 2024: \$500 Zelle from J.S.
- January 22, 2024: \$1,000 Zelle from Y.S.

98. **SUBJECT ACCOUNT 15** received no additional deposits. M.A. filed a fraud claim with her bank indicated that her cashier's check was the result of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wire from C.S. was also the result of a tech support or other elder fraud scam.

99. According to JP Morgan Chase, Y.S. reported that the Zelle transaction was the result of a scam. Based on my training and experience, and the investigation conducted to date, I believe that the Zelle's from M.C. and J.S. were also the result of a tech support or other elder fraud scam.

100. As of August 21, 2024, JP Morgan Chase is holding approximately \$8,000 in an internal JP Morgan Chase account associated with **SUBJECT ACCOUNT 15**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 15** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 15** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 16

101. On or around August 9, 2023, Lena Castle Inc was registered with the Virginia SCC. On or around January 24, 2024, Bank of America bank account number 435048231338 in the name of Lena Castle Inc was opened (“**SUBJECT ACCOUNT 16**”).

102. On February 18, 2024, LIANG sent the following WeChat message:

*Bank Name:bank of America
Account Name: Lena Castle Inc
Account number:435048231338
routing number for ach:051000017
routing number for wire:026009593*

*bank address: 4191 Dale Blvd
Woodbridge, VA 22193*

*company address:105 Oronoco st ste 300 Alexandria VA 22314
Online bank:ying1972luo
PW:Cal210038*

103. On February 7, 2024, a coconspirator sent the following WeChat message:

*Account Name: Lena Castle Inc
The payback account for this company principal
Bank Name :Community Federal Savings Bank
Account Name :KELSEA LIMITED
Account Number :8335427647
Currency :USD
Wires Number :026073008
Bank Address :810 Seventh Avenue, New York, NY 10019, US*

104. Between February 7, 2024 and February 22, 2024, **SUBJECT ACCOUNT 16** sent four wire transfers, totaling over \$240,000, to the Kelsea Limited ‘payback account.’

105. Prior to February 16, 2024, the balance of **SUBJECT ACCOUNT 16** was \$5,439.82. Between February 16, 2024 and March 5, 2024, **SUBJECT ACCOUNT 16** received seven deposits, totaling \$156,310, as detailed below:

- February 16, 2024: \$90,010 from D.P., residing in Oak Lawn, Illinois

- February 16, 2024: \$6,000 from J.S., holding a bank account at Desert Financial Credit Union
- February 20, 2024: \$25,000 from E.H., residing in Kailua Kona, Hawaii
- February 22, 2024: \$15,000 from J.T., holding a bank account at USAA Federal Savings
- February 23, 2024: \$1,500 from I.Q., residing in West Palm Beach, Florida
- March 5, 2024: \$17,800 from R.G., holding a bank account at Texas Bank

106. **SUBJECT ACCOUNT 16** only received two other deposits following February 26, 2024, which were returns of attempted check withdrawals. D.P., E.H, and I.Q. all filed IC3 complaints indicating that their wires were the results of a scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from J.S., J.T., and R.G. were the result of a tech support or other elder fraud scam.

107. As of August 15, 2024, Bank of America is holding approximately \$8,840.34 in an internal Bank of America account associated with **SUBJECT ACCOUNT 16**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 16** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 16** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 17

108. On or around October 19, 2023, BHB Products Trading Inc was registered with the Virginia SCC. On or around October 24, 2023, Truist bank account number 1470014663126 in the name of BHB Products Trading Inc was opened (“**SUBJECT ACCOUNT 17**”). Prior to January 9, 2024, the balance of **SUBJECT ACCOUNT 17** was \$237.84. **SUBJECT ACCOUNT 17** received the following deposits:

- January 10, 2024: \$35,000 from L.W., a 70-year-old residing in Austin, Texas
- January 11, 2024: \$32,000 from Noffsinger Physical Therapy LLC, located in Greenville, Kentucky
- January 11, 2024: \$88 from Chia Supplies Co Limited (one of the Fictitious Virginia Business Entities)

109. **SUBJECT ACCOUNT 17** did not receive any additional deposits. An IC3 complaint related to a \$65,000 deposit from J.S. on November 29, 2023 into **SUBJECT ACCOUNT 17** indicated that J.S. was the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from L.W. and Noffsinger Physical Therapy LLC were the result of a tech support or other elder fraud scam.

110. As of September 4, 2024, Truist is holding approximately \$31,604.97 in an internal Truist account associated with **SUBJECT ACCOUNT 17**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 17** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 17** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 18

111. On or around October 19, 2023, Amcor Plus One Wholesale Inc was registered with the Virginia SCC. On or around October 25, 2023, Truist bank account number 1470013063435 in the name of Amcor Plus One Wholesale Inc was opened (“**SUBJECT ACCOUNT 18**”). **SUBJECT ACCOUNT 18** received the following deposits:

- November 21, 2023: \$42,800 from B.E., an 86-year-old residing in Fremont, California
- November 21, 2023: \$49,000 from S.C., holding a bank account at PNC

112. **SUBJECT ACCOUNT 18** received \$500 in additional deposits. Based on my training and experience, and the investigation conducted to date, I believe that the cashier's checks from B.E. and S.C. were the result of a tech support or other elder fraud scam.

113. As of September 4, 2024, Truist is holding approximately \$29,760 in an internal Truist account associated with **SUBJECT ACCOUNT 18**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 18** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 18** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 19

114. On or around December 19, 2023, Chia Supplies Co Limited was registered with the Virginia SCC. On or around December 20, 2023, Truist bank account number 1470013876622 in the name of Chia Supplies Co Limited was opened ("**SUBJECT ACCOUNT 19**"). Prior to March 27, 2024, **SUBJECT ACCOUNT 19** had a balance of \$1,727.89.

SUBJECT ACCOUNT 19 received the following deposits:

- March 27, 2024: \$7,565 from G.V., an 88-year-old residing in San Francisco, California
- March 27, 2024: \$19,500 from Camp Van Vac LLC, located in Ely, Minnesota
- March 28, 2024: \$25,000 from H.R., a 71-year-old residing in Silver Spring, Maryland

115. **SUBJECT ACCOUNT 19** received an additional \$700.99 in deposits. H.R. reported to their local police department that they were the victim of a scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from G.V. and Camp Van Vac LLC were the result of a tech support or other elder fraud scam.

116. As of September 4, 2024, Truist is holding approximately \$25,218.42 in an internal Truist account associated with **SUBJECT ACCOUNT 19**. I have probable cause to

believe that the primary source of deposits into **SUBJECT ACCOUNT 19** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 19** constitute proceeds of the mail and wire fraud scheme.

SUBJECT ACCOUNT 20

117. On or around November 15, 2023, UJS Equipment Inc was registered with the Virginia SCC. On or around November 16, 2023, Truist bank account number 1210007787810 in the name of UJS Equipment Inc was opened (“**SUBJECT ACCOUNT 20**”). **SUBJECT ACCOUNT 20** received the following deposits:

- November 28, 2023: \$43,000 from J.D., a 76-year-old residing in Oklahoma City, Oklahoma
- November 30, 2023: \$9,700 from R.A., a 67-year-old residing in Bend, Oregon
- November 30, 2023: \$32,000 from P.C., a 70-year-old residing in Ellis, Kansas
- November 30, 2023: \$33,219 from J.S., a 69-year-old residing in Largo, Florida

118. **SUBJECT ACCOUNT 20** received an additional \$100 in deposits. J.S. reported to their local police department that they were the victim of a tech support scam. Based on my training and experience, and the investigation conducted to date, I believe that the wires from J.D., R.A., and P.C. were the result of a tech support or other elder fraud scam.

119. As of September 4, 2024, Truist is holding approximately \$73,419 in an internal Truist account associated with **SUBJECT ACCOUNT 20**. I have probable cause to believe that the primary source of deposits into **SUBJECT ACCOUNT 20** are victim funds, and the funds remaining in **SUBJECT ACCOUNT 20** constitute proceeds of the mail and wire fraud scheme.

CONCLUSION

120. Based on the facts contained herein, combined with the training and experience of the investigative team, I conclude that there is probable cause to believe that the **SUBJECT ACCOUNTS** contain proceeds of the wire and mail fraud scheme. The **SUBJECT ACCOUNTS** are therefore subject to seizure and forfeiture pursuant to the statutory authority set forth above.

121. Based on the foregoing, it is requested that seizure warrants be issued for the funds contained within the **SUBJECT ACCOUNTS** identified in this affidavit pursuant to the authority cited above.


Samantha
Wendt

Digitally signed by Samantha
Wendt
Date: 2024.09.12 10:55:37
-04'00'

Samantha Wendt
Special Agent
Federal Bureau of Investigation

Attested to me in accordance with the requirements of Fed. R. Crim. P. 4.1 via telephone on September 13, 2024.


Lindsey R Vaala

Digitally signed by Lindsey R
Vaala
Date: 2024.09.13 12:46:30
-04'00'

The Honorable Lindsey R. Vaala
United States Magistrate Judge